Ash Notes
Chapter 2

Wiliam M. Faucette

Let E/F be a finite field extension. Let $x \in E$. Let $m(x)$ be the F-linear transformation $y \mapsto m(x)y = xy$

Definition. The **norm** of x is $N_{E/F}(x) = \det(m(x))$ and the **trace** of x is $T_{E/F}(x) = \operatorname{tr}(m(x))$.

Definition. Let $A(x)$ be the matrix for $m(x)$ with respect to some basis of E over F. The norm of x is the determinant of $A(x)$ and the trace of x is the trace of $A(x)$.

The **characteristic polynomial** of x is the characteristic polynomial of the matrix $A(x)$. That is,

$$\operatorname{char}_{E/F}(x) = \det(XI - A(x)) .$$

Fact: The second coefficient of $\operatorname{char}_{E/F}(x)$ is $-T(x)$ and the constant coefficient is $(-1)^n N(x)$.

Fact: Trace is additive. Norm is multiplicative.

Proposition. *Let $\min(x,F)$ be the minimal polynomial of x over F and let $r = [E : F(x)]$. Then*

$$\operatorname{char}_{E/F}(x) = [\min(x,F)]^r .$$

Corollary. *Let $[E : F] = n$ and $[F(x) : F] = d$. Let $x_1, \ldots, x_d$ be the roots of $\min(x,F)$, counting multiplicity, in a splitting field. Then*

$$N(x) = \left(\prod_{i=1}^{d} x_i\right)^{n/d}, \quad T(x) = \frac{n}{d}\sum_{i=1}^{d} x_i, \quad \operatorname{char}_{E/F}(x) = \left[\prod_{i=1}^{d}(X - x_i)\right]^{n/d} .$$

Proposition. *Let E/F be a separable extension of degree n, and let $\sigma_1, \ldots, \sigma_n$ be the distinct F-embeddings (that is, F-monomorphisms) of E into an algebraic closure of E, or equally well into a normal extension L of F containing E. Then*

$$N_{E/F}(x) = \prod_{i=1}^{n} \sigma_i(x), \quad T_{E/F}(x) = \sum_{i=1}^{n} \sigma_i(x), \quad \operatorname{char}_{E/F}(x) = \prod_{i=1}^{n}(X - \sigma_i(x)).$$

Proposition. *If $F \leq K \leq E$, where E/F is finite and separable, then*

$$T_{E/F} = T_{K/F} \circ T_{E/K} \quad \textit{and} \quad N_{E/F} = N_{K/F} \circ N_{E/K}.$$

Proposition. *If E/F is a finite separable extension, then the trace $T_{E/F}(x)$ cannot be 0 for every $x \in E$.*

This is a result of Dedekind's Lemma.

Remark. This proposition can be restated as: If E/F is finite and separable, the *trace form,* that is, the bilinear form $(x, y) \to T_{E/F}(xy)$, is nondegenerate.

Example. Let $x = a + b\sqrt{m} \in \mathbb{Q}(\sqrt{m})$, where m is a square-free integer.

The Galois group of the extension $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$ consists of the identity and the automorphism $\sigma(a + b\sqrt{m}) = a - b\sqrt{m}$. Then

$$T(x) = x + \sigma(x) = 2a \quad \text{and} \quad N(x) = x\sigma(x) = a^2 - mb^2.$$

1. Basic Setup for Algebraic Number Theory

A and integral domain with fraction field K. L is a finite separable extension of K and B is the ingegral closure of A in L.

$$\begin{array}{ccc} L & \longrightarrow & B \\ \downarrow & & \downarrow \\ K & \longrightarrow & A \end{array}$$

In the most important case, $A = \mathbb{Z}$, $K = \mathbb{Q}$, L is a number field, and B is the ring of algebraic integers in L.

Proposition. *If $x \in B$, then the coefficients of* $\mathrm{char}_{L/K}(x)$ *and* $\min(x, K)$ *are integral over A. In particular, $T_{L/K}(x)$ and $N_{L/K}(x)$ are integral over A. If A is integrally closed, then the coefficients belong to A.*

Corollary. *Assume A integrally closed, and let $x \in L$. Then x is integral over A, that is, $x \in B$, if and only if the minimal polynomial of x over K has coefficients in A.*

Corollary. *An algebraic integer a that belongs to $\mathbb{Q}$ must in fact belong to $\mathbb{Z}$.*

2. Quadratic Extensions of the Rationals

Let m be a square-free integer and $L = \mathbb{Q}(\sqrt{m})$.

The minimal polynomial over $\mathbb{Q}$ of the element $a + b\sqrt{m}$ (with $a, b \in \mathbb{Q}$) is $X^2 - 2aX + a^2 - mb^2$. So $a + b\sqrt{m}$ is an algebraic integer if and only if $2a$ and $a^2 - mb^2$ lie in $\mathbb{Z}$.

$$(2a)^2 - 4(a^2 - mb^2) = 4mb^2 = (2b)^2 m \in \mathbb{Z}$$

If $2b \notin \mathbb{Z}$, then any prime in the denominator of b cannot be canceled by m since m is square-free. So, in this case, $2b$ must also be in $\mathbb{Z}$.

Proposition. *The set B of algebraic integers of $\mathbb{Q}(\sqrt{m})$, m square-free, can be described as follows.*

(i) *If $m \not\equiv 1 \pmod 4$, then B consists of all $a + b\sqrt{m}$, $a, b \in \mathbb{Z}$.*

(ii) *If $m \equiv 1 \pmod 4$, then B consists of all $\frac{u}{2} + \frac{v}{2}\sqrt{m}$, $u, v \in \mathbb{Z}$ with $u \equiv v \pmod 2$.*

Proposition. *There is a basis for L/K consisting entirely of elements of B. (For any element in L, a nonzero multiple (by an element of A) of that element is in B.*

Corollary. *If $x \in L$, then there is a nonzero element $a \in A$ and an element $y \in B$ such that $x = y/a$. In particular, L is the fraction field of B.*

Theorem. *Let (x, y) be a nondegenerate symmetric bilinear form on an n-dimensional vector space V. If $x_1, \ldots, x_n$ is a basis for V, then there is a basis $y_1, \ldots, y_n$ for V, the **dual basis referred to** V, such that $(x_i, y_j) = \delta_{ij}$.*

3. The Discriminant

Definition. If $n = [L : K]$, the **discriminant** of the n-tuple $x = (x_1, \ldots, x_n)$ of elements of L is

$$D(x) = \det\big(T_{L/K}(x_i x_j)\big)\,.$$

Form the matrix with $a_{ij} = T_{L/K}(x_i x_j)$ and take the determinant.

Lemma. *If $y = Cx$, where C is an n by n matrix over K and x and y are n-tuples written as column vectors, then $D(y) = (\det C)^2 D(x)$.*

Proof. If $C = [c_{ij}]$, then $y_r = \sum_{i=1}^{n} c_{ri} x_i$ and

$$\begin{aligned} y_r y_s &= \left(\sum_{i=1}^{n} c_{ri} x_i \right) \left(\sum_{j=1}^{n} c_{sj} x_j \right) \\ &= \sum_{i,j=1}^{n} c_{ri} x_i x_j c_{sj} \end{aligned}$$

So,

$$\begin{aligned} T(y_r y_s) &= T\left(\sum_{i,j=1}^{n} c_{ri} x_i x_j c_{sj} \right) \\ &= c_{ri} T\left(\sum_{i,j=1}^{n} x_i x_j \right) c_{sj}, \end{aligned}$$

so,

$$(T(y_r y_s)) = C(T(x_i x_j))C^T$$

The result follows by taking the determinant. □

Lemma. *Let $\sigma_1, \ldots, \sigma_n$ be the distinct K-embeddings of L into an algebraic closure of L. Then $D(x) = [\det(\sigma_i(x_j))]^2$.*

Proof.

$$T(x_i x_j) = \sum_k \sigma_k(x_i x_j) = \sum_k \sigma_k(x_i)\sigma_k(x_j),$$

so if $H = [\sigma_i(x_j)]$, then $(T(x_i x_j)) = H^T H$. Now take determinants. □

Proposition. *If $x = (x_1, \ldots, x_n)$, then the x_i form a basis for L over K if and only if $D(x) \neq 0$.*

Proof. See Chapter 2, page 9. □

Proposition. *Assume that $L = K(x)$, and let f be the minimal polynomial of x over K. Let D be the discriminant of the basis $1, x, x^2, \ldots, x^{n-1}$ over K, and let $x_1, \ldots, x_n$ be the roots of f in a splitting field, with $x_1 = x$. Then $D = \prod_{i<j}(x_i - x_j)^2$, the discriminant of the polynomial f.*

Proof. Let σ_i be the K-embedding that takes x to x_i, $i = 1, \dots, n$. Then the matrix $\sigma_i(x^j) = x_i^j$, $0 \leq j \leq n-1$. Then D is the square of the determinant of the matrix

$$V = \begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{bmatrix}.$$

But $\det(V)$ is a Vandermonde determinant, whose value is $\prod_{i<j}(x_i - x_j)$. □

Corollary. *Under the hypothesis of the last proposition*

$$D = (-1)^{\binom{n}{2}} N_{L/K}(f'(x))$$

where f' is the derivative of f.

Proof. Let $c = (-1)^{\binom{n}{2}}$. Then

$$D = \prod_{i<j}(x_i - x_j)^2 = c\prod_{i \neq j}(x_i - x_j) = c\prod_i \prod_{j \neq i}(x_i - x_j).$$

But $f(X) = (X - x_1)\cdots(X - x_n)$, so

$$f'(X) = \sum_k \prod_{j \neq k}(X - x_j),$$

and

$$f'(x_i) = \sum_k \prod_{j \neq k}(X - x_j)|_{x_i} = \prod_{j \neq i}(x_i - x_j).$$

So,

$$D = c\prod_{i=1}^n f'(x_i).$$

But,

$$f'(x_i) = f'(\sigma_i(x)) = \sigma_i(f'(x)),$$

so

$$D = cN_{L/k}(f'(x)).$$

□

Remark. In the $AKLB$ setup with $[L : K] = n$, suppose that B turns out to be a free A-module of rank n. A basis for this module is an *integral basis* of B (or of L). This is a basis for L over K. Such a basis always exists when L is a number field. The discriminant is the same for all integral bases. It is called the *field discriminant*.

Theorem. *If A is integrally closed, then B is a submodule of a free A-module of rank n. If A is a PID, then B itself is free of rank n over A, so B has an integral basis.*

Proof. Let $x_1, \ldots, x_n$ be any basis for L over K consisting of elements of B and let $y_1, \ldots, y_n$ be the dual basis referred to L. If $z \in B$, then we can write $z = \sum_j a_j y_j$ with $a_j \in K$. We know that the trace of x_z belongs to A, and we also hve

$$T(x_i z) = T\left(\sum_{j=1}^{n} a_j x_i y_j\right) = \sum_{j=1}^{n} a_j T\left(x_i y_j\right) = \sum_{j=1}^{n} a_j \delta_{ij} = a_i.$$

Thus, each a_i belongs to A, so that B is an A-submodule of the free A-module $\oplus_{j=1}^{n} A y_j$. Moreover, B contains the free A-module $\oplus_{j=1}^{n} A x_j$. Consequently, if A is a PID, then B is free over A of rank n. $\square$

Corollary. *The set B if algebraic integers in any number field L if a free $\mathbb{Z}$-module of rank $n = [L : \mathbb{Q}]$. Therefore B has an integral basis. The discriminant is the same fo every integral basis.*

Proof. Take $A = \mathbb{Z}$ in the theorem to show that B has an integral basis. The transformation matrix C between two integral bases is invertible, and both C and C^{-1} have rational integral coefficients. Take determinants to conclude that $\det(C)$ is a unit in $\mathbb{Z}$. But then D is well-defined for all integral bases. $\square$

Remark. An invertible matrix C with coefficients in $\mathbb{Z}$ is **unimodular** if C^{-1} also has coefficients in $\mathbb{Z}$. We just saw that unimodular matrix has determinant ± 1. Conversely, a matrix over $\mathbb{Z}$ with determinant ± 1 is unimodular, by Cramer's rule.

Theorem. *Let B be the algebraic integers of $\mathbb{Q}(\sqrt{m})$, where m is a square-free integer.*

(i) *If $m \not\equiv 1 \pmod 4$, then 1 and $\sqrt{m}$ form an integral basis, and the field discriminant is $d = 4m$.*

(ii) *If $m \equiv 1 \pmod 4$, then 1 and $(1 + \sqrt{m})/2$ form an integral basis, and the field discriminant is $d = m$.*

Proof. (i) The numbers 1 and $\sqrt{m}$ span B over $\mathbb{Z}$, and the are linearly independent. The trace of $a + b\sqrt{m}$ is $2a$, so the field discriminant is

$$\begin{vmatrix} 2 & 0 \\ 0 & 2m \end{vmatrix} = 4m.$$

[Recall: $D(x) = \det\big(T_{L/\mathbb{Q}}(x_i x_j)\big)$]]

(ii) The numbers 1 and $(1 + \sqrt{m})/2$ span B over $\mathbb{Z}$, and the are linearly independent. The trace of $a + b\sqrt{m}$ is $2a$, so the field discriminant is

$$\begin{vmatrix} 2 & 1 \\ 1 & (1+m)/2 \end{vmatrix} = m.$$

[Recall: $D(x) = \det\big(T_{L/\mathbb{Q}}(x_i x_j)\big)$]]

□